5.2 Hardware Trojan

In terms of **Hardware security**, It is a malicious modification of the circuitry of an IC chip. It is done during the design or fabrication of chip i.e. The chip is modified without the possible knowledge of the person who designed it.

It is sometimes also known as **‘HT'**. A Hardware Trojan or HT is something, a piece of hardware, which is hiding inside another larger piece of hardware. It wakes up at unpredictable times and does something malicious which is again unpredictable with respect to user.

A Hardware Trojan (HT) is categorized by two things -

1. Physical Representation (i.e. how it behaves, how it looks like)
2. It's behavior (i.e. how it shows up and what are its effects)

Properties of a Hardware Trojan -

1. It can take place pre or post manufacturing.
2. It is inserted by some intellectual adversary.
3. It is extremely small hardware overhead.
4. It is Stealthy and nearly Impossible to detect
5. It causes IC to malfunction in-field.

Affects of a Hardware Trojan if it's placed inside a chip -

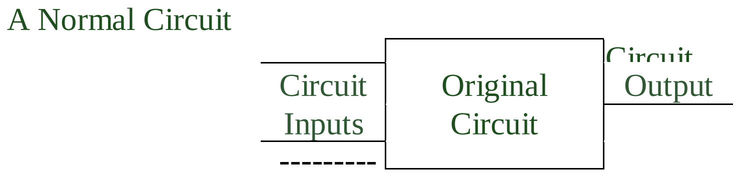
1. Potentially disastrous consequences.
2. Loss of human life or property.

Whenever the **HT** wakes up , the entire activity that the Trojan performs or executes is known as **payload**.

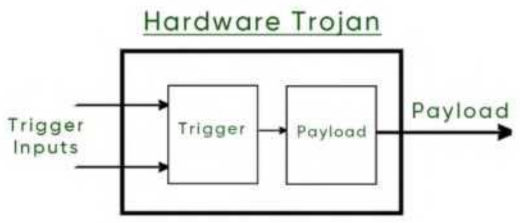
Components of a Hardware Trojan -

It contains a **trigger** and a **payload**

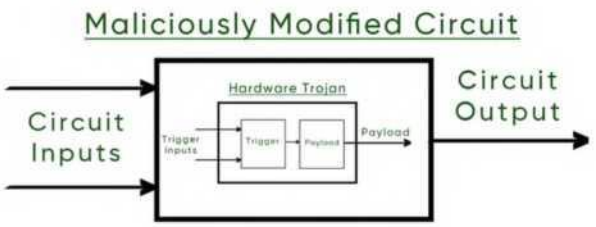
1. Trigger - Trigger decides when the Hardware Trojan or HT will wake up and
2. Payload - Payload decides what will happen when the Trojan will wake up.



(a) A Typical Circuit



(b) A Hardware Trojan



(c) A Maliciously Modified Circuit

It is maliciously placed in the original circuit. User doesn't know about this because most of the time circuit will behave normally, but sometimes it behaves unpredictably / maliciously whenever it wakes up. As shown in the above diagrams.

Reasons why it might get inserted into a chip -

1. Prevalence of IP(Intellectual Property Core) based design.
2. Routine use of CAD tools for EDA Vendors.
3. Fabless manufacturing model (i.e. We do not design it ourselves we give someone to design it, there might something happen)
4. Loss of control over design and manufacture, etc.

Do Hardware Trojan Really Exist ?

1. No Concrete proof of Hardware Trojan is obtained as yet.
2. Tampering masks in fab is not easy, it is a complex process.
3. Reverse engineering of a single IC can take months.

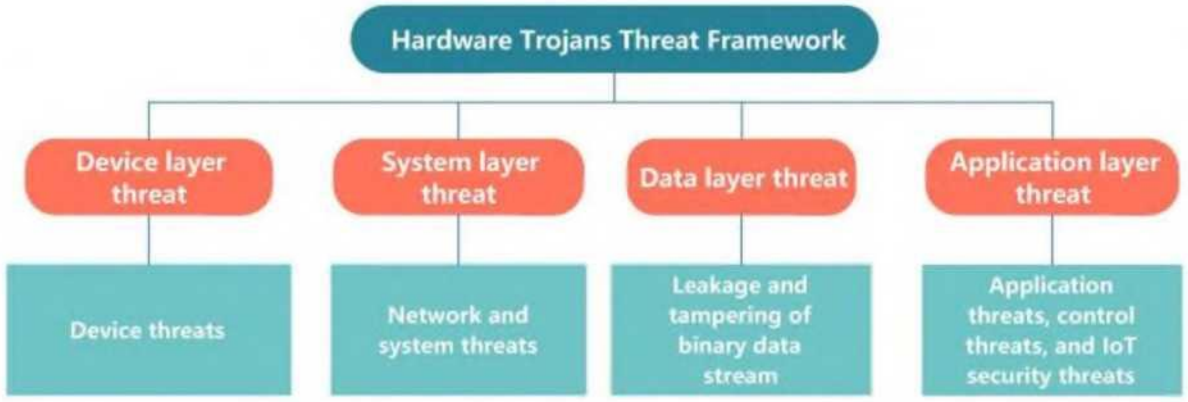

Hardware Trojans Threat Framework
Device layer threat
System layer threat
Data layer threat
Application layer threat
Device threats
Network and system threats
Leakage and tampering of binary data stream
Application threats, control threats, and IoT security threats

Fig: Hardware Trojans Threat Framework

Device Layer Threat of Hardware Trojans

Device layer threat is defined as device damage that is caused by HTs. Similar to the fact that information depends on a physical carrier, HTs are presented on the chip in the form of additional physical implants or tampering with hardware parameters, and the chip relies on the device as a carrier. Therefore, malicious tampering with chip hardware means that HTs cause physical damage through the device. This physical destructiveness is often invisible on visual inspection but illustrates the concealment of HT. This kind of implantability or parasitics best reflects the threat features at this layer, since the bottom layer of the circuit device is the primary goal of HT implantation.

System Layer Threat of Hardware Trojans

The system layer threat manifests as interference to network and system. Starting from this layer, the destructiveness brought by HTs has been enhanced. Software trojans have similarities with HT, which is, they are both camouflaged. Software trojans are malicious codes that are parasitic on software programs, but, on the surface, they are consistent with normal software. The user enters private information, such as account number and password, into the infected malware window, and the attacker remotely controls the software to illegally receive the data. When certain trojan programs respond to user requests, they continue to pop up error prompt windows to DoS, resulting in failure to complete normal program use. There have not been many examples to show the damage to the software system due to the insufficiency of detection technology at this stage and the limitations of HT design methods. However, with the development of technology and the deepening of research in the future, the malicious influence of HTs on software systems is not impossible. Boraten et al. designed a target-activated sequential payload (TASP) HT on NoC, which, in conjunction with a counter based on the finite state machine (FSM), causes irreversible failures on multiple links.

Data Layer Threat of Hardware Trojans

The data layer threat can generally be understood as the risk of attacks on data, identity, and privacy information. From the root cause, it is reflected as HTs leaking and tampering with the integrity of the binary stream data on the original circuit. A simple HT that is based on electromagnetic leakage was a case of data layer threat. When HT was activated, the acoustic signals were used to express the bits of the key, and then radiated out by radio wave. An attacker used an ordinary radio to receive these signals, interpreting the key through the different sounds expressed by these signals. The adversary implants HT backdoors to attack the biochip used in medical diagnosis, and the identity information and privacy information of the patient's condition can be easily obtained illegally through reagent residues. There is an example of HT on the new-style artificial intelligence (AI) chips.

Application Layer Threat of Hardware Trojans

Application layer threat emphasizes application threats, control threats, and IoT security threats. A more obvious feature of threats at the layer is the security threats generated under the influence of interaction with end-users. Therefore, in the IoT, smart devices, driverless cars, and robots that rely on SoC devices cannot do without sensors to sense operations. If they suffer from HT security vulnerabilities, they will put other devices in the shared network at the same risk. Even chips with similar loopholes on atmospheric observation radars produce the same destruction. Hackers only needed to launch an HT attack on the joint test action group (JTAG) interface on the printed circuit boards (PCB) and illegally accessed the memory through the data bus to obtain the authorization to modify the data. On NoC, there was a kind of HT that can launch bandwidth DoS attacks. This attack phenomenon slowed down communication, decreased application performance, and affected system reliability [59]. The above three cases illustrate the concept of application threats for observation interaction, interface interaction, and communication interaction.